An Illustrative Study on Cloud Computing

R. Madhubala

Abstract— ***"Cloud" computing – a relatively recent term, defines the paths ahead in computer science world. Being built on decades of research it utilizes all recent achievements in virtualization, distributed computing and utility computing. This paper is about the definition of cloud, architecture and security issues of cloud***

Keywords— ***Cloud, virtualization, security, infrastructure***

I. INTRODUCTION

Cloud computing is a paradigm that focuses on sharing data and computations over a scalable network of nodes. Basically cloud is a metaphor for internet and is an abstraction for the complex infrastructure it conceals.

Cloud is the convergence and evolution of several concepts from virtualization, distributed application design, grid, and enterprise IT management to enable a more flexible approach for deploying and scaling applications. Cloud infrastructures enable companies to cut costs by outsourcing computations on-demand. However, clients of cloud computing services currently have no means of verifying the confidentiality and integrity of their data and computation. Cloud promises real costs savings and agility to customers.

Through cloud computing, a company can rapidly deploy applications where the underlying technology components can expand and contract with the natural ebb and flow of the business life cycle. Traditionally, once an application was deployed it was bound to a particular infrastructure, until the infrastructure was upgraded. The result was low efficiency, utilization, and flexibility.

Cloud enablers, such as virtualization and grid computing, allow applications to be dynamically deployed onto the most suitable infrastructure at run time. This elastic aspect of cloud computing allows applications to scale and grow without needing traditional 'fork-lift' upgrades.

It is a style of computing in which IT-related capabilities are provided "as a service", allowing users to access technology-enabled services from the Internet (i.e., the Cloud) without knowledge of, expertise with, or control over the technology infrastructure that supports them.

II. ARCHITECTURE OF CLOUD COMPUTING

Cloud computing architecture comprised of essential characteristics, cloud service models, and cloud deployment models. They are summarized in visual form in Figure 1 and explained in detail below.

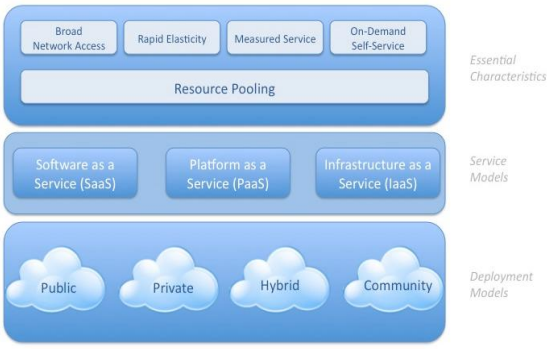

Fig 1 – Architecture of Cloud Computing

A. Essential Characteristics of Cloud Computing

Cloud services exhibit five essential characteristics that demonstrate their relation to and differences from, traditional computing approaches:

1) **On-demand self-service**: A consumer can unilaterally provision computing capabilities such as server time and network storage as needed automatically, without requiring human interaction with a service provider.

2) **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs) as well as other traditional or cloud based software services.

3**) Resource pooling**. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a degree of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. Even private clouds tend to pool resources between different parts of the same organization.

4) **Rapid elasticity**. Capabilities can be rapidly and elastically provisioned — in some cases automatically — to quickly scale out; and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

5**) Measured service**. Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, or active user accounts). Resource usage can be monitored, controlled, and reported — providing transparency for both the provider and consumer of the service.

Manuscript Received on December 14, 2011

Mrs.R.Madhubala, Asst. Professor, MCA Department,Ethiraj College for Women, Chennai– 600 008, India, (E-mail: balamadh@gmail.com)

It is important to recognize that cloud services are often but not always utilized in conjunction with, and enabled by, virtualization technologies. There is no requirement, however, that ties the abstraction of resources to virtualization technologies and in many offerings virtualization by hypervisor or operating system container is not utilized.

B. Service Model in Cloud

Cloud service delivery is divided among three archetypal models and various derivative combinations. The three fundamental classifications are often referred to as the "SPI Model", where 'SPI' refers to ***Software, Platform or Infrastructure*** (as a Service), respectively — defined. The following fig 2 refers the cloud service models.

1) **Cloud Software as a Service (SaaS) :** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email

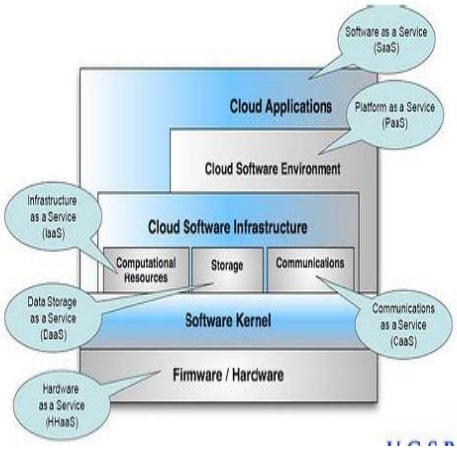

Fig 2 – Cloud Service Models

2) **Cloud Platform as a Service (PaaS)** : The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider (eg. configurations)

3) **Cloud Infrastructure as a Service (IaaS)**: The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.(e.g., host firewalls)

C. Cloud Deployment Models

Regardless of the service model utilized (SaaS, PaaS, or IaaS) there are four deployment models for cloud services, with derivative variations that address specific requirements are depicted in fig 3:

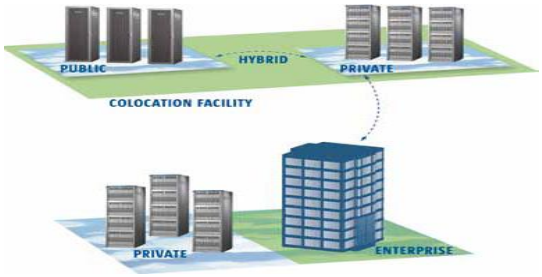

Fig 3 – Cloud Deployment Models

1) ***Public Cloud***: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

2) ***Private Cloud***: The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off premises.

3) ***Community Cloud***: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and may exist on-premises or off-premises.

4) ***Hybrid Cloud***: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability

It is important to note that there are derivative cloud deployment models emerging due to the maturation of market offerings and customer demand. An example of such is virtual private clouds — a way of utilizing public cloud infrastructure in a private or semi-private manner and interconnecting these resources to the internal resources of a consumers' data center, usually via virtual private network (VPN) connectivity. In the forthcoming session, the security of cloud computing are discusses

III. SECURITY OF CLOUD COMPUTING

Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties.

An organization's security posture is characterized by the maturity, effectiveness, and completeness of the risk-adjusted security controls implemented. These controls are implemented in one or more layers ranging from the facilities (physical security), to the network infrastructure (network security), to the IT systems (system security), all the way to the information and applications (application security).. The security responsibilities of both the provider and the consumer greatly differ between cloud service models.

Cloud computing is the cost efficiencies afforded by economies of scale, reuse, and standardization. To bring these efficiencies to bear, cloud providers have to provide services that are flexible enough to serve the largest customer base possible, maximizing their addressable market. Integrating security into these solutions is often perceived as making them more rigid. This rigidity often manifests in the inability to gain parity in security control deployment in cloud environments compared to traditional IT.

The figure 4 below illustrates the issues: in service models:

1) In SaaS environments the security controls and their scope are negotiated into the contracts for service; service levels, privacy, and compliance are all issues to be dealt with legally in contracts.

2) In an IaaS offering, while the responsibility for securing the underlying infrastructure and abstraction layers belongs to the provider, the remainder of the stack is the consumer's responsibility.

3) PaaS offers a balance somewhere in between, where securing the platform itself falls onto the provider, but securing the applications developed against the platform and developing them securely, both belong to the consumer.

Cloud computing providing unlimited infrastructure to store and execute customer data and program. As customers you do not need to own the infrastructure, they are merely accessing or renting; they can forego capital expenditure and consume resources as a service, paying instead for what they use.

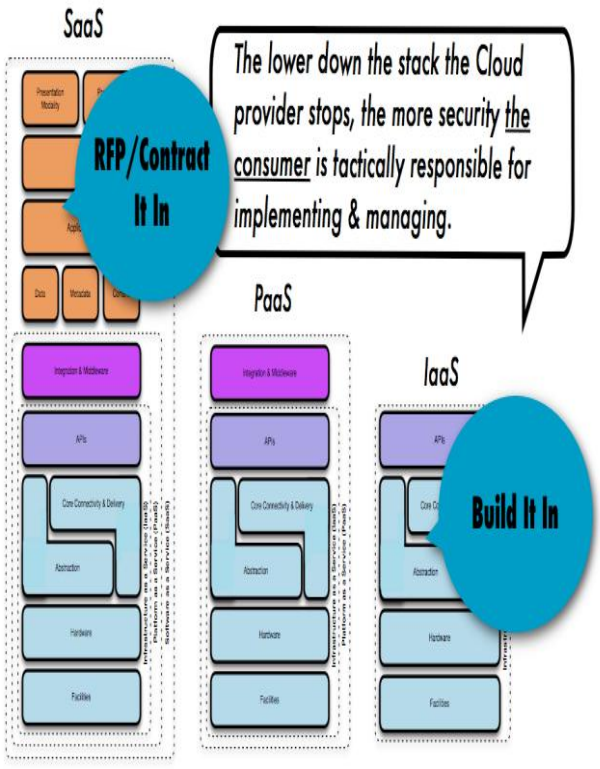

Fig 4 - Security Gets Integrated

A. Principle elements for securing the Cloud: Secure Identity, Information and Infrastructure

Public cloud computing requires a security model that reconciles scalability and multi-tenancy with the need for trust. In the figure 5 the enterprises move their computing environments with their identities, information and infrastructure to the cloud; they must be willing to give up some level of control. To do that, they must be able to trust cloud systems and providers, and verify cloud processes and events. Important building blocks of trust and verification relationships include access control, data security, compliance and event management – all security elements well understood by IT departments today, implemented with existing products and technologies, and extendable into the cloud.

Fig 5 – Principle elements of Cloud Computing

i) Identity security

End-to-end identity management, third-party authentication services, and federated identity will become a key element of cloud security. Identity security preserves the integrity and confidentiality of data and applications while making access readily available to appropriate users. Support for these identity management capabilities for both users and infrastructure components will be a major requirement for cloud computing, and identity will have to be managed in ways that build trust. It will require:

a**. Strong authentication**: Cloud computing must move beyond weak username-and-password authentication if it is going to support the enterprise. This will mean adopting techniques and technologies that are already standard in enterprise IT such as strong authentication (multi-factor authentication with one-time password technology), federation within and across enterprises, and risk-based authentication that measures behavior history, current context and other factors to assess the risk level of a user request. Additional tiering of authentication will be essential to meet security SLAs, and utilizing a risk-based authentication model that is largely transparent to the users will actually reduce the need for broader federation of access controls.

b. More **granular authorization**: Authorization can be coarse-grained within an enterprise or even a private cloud, but in order to handle sensitive data and compliance requirements, public clouds will need granular authorization capabilities (such as role-based controls and IRM) that can be persistent throughout the cloud infrastructure and the data's lifecycle.

ii). Information Security

In the cloud, that protective barrier that secures infrastructure is diffused. To compensate, security will have to become information centric. The data needs its own security that travels with it and protects it. It will require:

a. Data isolation: In multi-tenancy situations, data must be held securely in order to protect it when multiple customers use shared resources. Virtualization, encryption and access control will be workhorses for enabling varying degrees of separation between corporations, communities of interest and users.
   In the near future, data isolation will be more important and executable for IAAS, than perhaps for PAAS and SAAS.
b. More granular data security: As the sensitivity of information increases, the granularity of data classification enforcement must increase. In current data center environments, granularity of role-based access control at the level of user groups or business units is acceptable in most cases because the information remains within the control of the enterprise itself. For information in the cloud, sensitive data will require security at the file, field, or even block level to meet the demands of assurance and compliance.
c. Consistent data security: There will be an obvious need for policy-based content protection to meet the enterprise's own needs as well as regulatory policy mandates. For some categories of data, information centric security will necessitate encryption in transit and at rest, as well as management across the cloud and throughout the data lifecycle.
d. Effective data classification: Cloud computing imposes a resource trade-off between high performance and the requirements of increasingly robust security. Data classification is an essential tool for balancing that equation. Enterprises will need to know what data is important and where it is located as prerequisites to making performance cost/benefit decisions, as well as ensuring focus on the most critical areas for data loss prevention procedures.
e. Information rights management: IRM is often treated as a component of identity, a way of setting broad-brush controls on which users have access to which data. But more granular data-centric security requires that policies and control mechanisms on the storage and use of information be associated directly with the information itself.
f. Governance and compliance: A key requirement of corporate information governance and compliance is the creation of management and validation information – monitoring and auditing the security state of the information with logging capabilities. Here, not only is it important to document access and denials to data, but to ensure that IT systems are configured to meet security specifications and have not been altered. Expanding retention policies for data policy compliance will also become an essential cloud capability. In essence, cloud computing infrastructures must be able to verify that data is being managed per the applicable local and international regulations (such as PCI and HIPAA) with appropriate controls, log collection and reporting.

iii) Infrastructure security

The foundational infrastructure for a cloud must be inherently secure whether it is a private or public cloud or whether the service is SAAS, PAAS or IAAS. It will require:

a. Inherent component-level security: The cloud needs to be architected to be secure, built with inherently secure components, deployed and provisioned securely with strong interfaces to other components, and, finally, supported securely, with vulnerability-assessment and change-management processes that produce management information and service-level assurances that build trust. For these flexibly deployed components, device fingerprinting to ensure secure configuration and state will also be an important security element, just as it is for the data and identities themselves.

b. More granular interface security: The points in the system where hand-offs occur – user-to-network, server-to application require granular security policies and controls that ensure consistency and accountability. Here, either the end-to-end system needs to be proprietary, a de facto standard, or a federation of vendors offering consistently deployed security policies.

c. Resource lifecycle management: The economics of cloud computing are based on multi-tenancy and the sharing of resources. As a customer's needs and requirements change, a service provider must provision and decommission those resources – bandwidth, servers, storage, and security – accordingly. This lifecycle process must be managed for accountability in order to build trust.

IV. CONCLUSIONS

Cloud computing promises to change the economics of the data center, but before sensitive and regulated data move into the public cloud, issues of security standards and compatibility must be addressed including strong authentication, delegated authorization, key management for encrypted data, data loss protections, and regulatory reporting. All are elements of a secure identity, information and infrastructure model, and are applicable to private and public clouds as well as to IAAS, PAAS and SAAS services. In the development of public and private clouds, enterprises and service providers will need to use these guiding principles to selectively adopt and extend security tools and secure products to build and offer end-to-end trustworthy cloud computing and services.

Fortunately, many of these security solutions are largely available today and are being developed further to undertake increasingly seamless cloud functionalities.

REFERENCES

1. S. M. Metev and Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, A Berkeley View of Cloud Computing, February 10, 2009
2. Andy Bechtolsheim, Chairman & Co-founder, Arista Networks, Cloud Computing, November 12th, 2008
3. Introduction to Cloud Computing Architecture, Sun Microsystems, Inc.
4. An Oracle White Paper in Enterprise Architecture, August 2009 Architectural Strategies for Cloud Computing .
5. David Chappell, a short introduction to cloud Platforms, An enterprise-oriented view, august 2008,

AUTHOR PROFILE

Mrs.R.Madhubala, Asst. Professor, Ethiraj College for women, Chennai, India. Has 10 years of experience in IT department.